



DEPARTMENT OF COMMERCE

National Institute of Standards and Technology

[Docket No.: 230816-0196]

National Cybersecurity Center of Excellence (NCCoE) *Accelerate Adoption of Digital Identities on Mobile Devices*

AGENCY: National Institute of Standards and Technology, Department of Commerce.

ACTION: Notice.

SUMMARY: The National Institute of Standards and Technology (NIST) invites organizations to provide letters of interest describing technical expertise and products to support and demonstrate International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 18013-5 and ISO/IEC 18013-7 standards capabilities for the *Accelerate Adoption of Digital Identities on Mobile Devices* project. This notice is the initial step for the National Cybersecurity Center of Excellence (NCCoE) in collaborating with technology companies to address cybersecurity challenges identified under the *Accelerate Adoption of Digital Identities on Mobile Devices* project. Participation in the project is open to all interested organizations.

DATES: Collaborative activities will commence as soon as enough completed and signed letters of interest have been returned to address all the necessary components and capabilities, but no earlier than [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE **FEDERAL REGISTER**].

ADDRESSES: The NCCoE is located at 9700 Great Seneca Highway, Rockville, MD 20850. Letters of interest must be submitted to mdl-nccoe@nist.gov or via hardcopy to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Interested parties can access the letter of interest request by visiting <https://www.nccoe.nist.gov/projects/digital-identities-mdl> and completing the

letter of interest webform. NIST will announce the completion of the selection of participants and inform the public that it is no longer accepting letters of interest for this project at <https://www.nccoe.nist.gov/projects/digital-identities-mdl>. Organizations whose letters of interest are accepted in accordance with the process set forth in the **SUPPLEMENTARY INFORMATION** section of this notice will be asked to sign an NCCoE consortium Cooperative Research and Development Agreement (CRADA) with NIST. An NCCoE consortium CRADA template can be found at:

<https://www.nccoe.nist.gov/publications/other/nccoe-consortium-crada-example>.

FOR FURTHER INFORMATION CONTACT: Ketan Mehta via email at mdl-nccoe@nist.gov; by phone at (301) 975-8405; or by mail to National Institute of Standards and Technology, NCCoE; 9700 Great Seneca Highway, Rockville, MD 20850. Additional details about the *Accelerate Adoption of Digital Identities on Mobile Devices* project are available at <https://www.nccoe.nist.gov/projects/digital-identities-mdl>.

SUPPLEMENTARY INFORMATION:

Background: The NCCoE, part of NIST, is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The NCCoE brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) and Operational Technology (OT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT and OT assets, the NCCoE will enhance trust in U.S. IT and OT communications, data, and storage systems; reduce risk for companies and individuals using IT and OT systems; and encourage development of innovative, job-creating cybersecurity products and services.

Process: NIST is soliciting responses from all sources of relevant security capabilities (see below) to enter into an NCCoE Cooperative Research and Development Agreement

(CRADA) to provide technical expertise and products to support and demonstrate ISO/IEC 18013-5 and ISO/IEC 18013-7 standards capabilities for the *Accelerate Adoption of Digital Identities on Mobile Devices* project. The full project can be viewed at: <https://www.nccoe.nist.gov/projects/digital-identities-mdl>.

Interested parties can access the request for a letter of interest template by visiting the project website at <https://www.nccoe.nist.gov/projects/digital-identities-mdl> and completing the letter of interest webform. On completion of the webform, interested parties will receive access to the letter of interest template, which the party must complete, certify as accurate, and submit to NIST by email or hardcopy. NIST will contact interested parties if there are questions regarding the responsiveness of the letters of interest to the project objective or requirements identified below. NIST will select participants who have submitted complete letters of interest on a first come, first served basis. The selection of participants who are Verifiers (aka, Relying Parties) will also be on a first come, first served basis; however, NIST will only select up to two Verifiers per transaction type. There are five transaction types which are described in Section 4 of the project description. Moreover, NIST may give preference to Verifiers that propose use of mobile driver's license (mDL) as well as other documents. Participants who are Verifiers may submit multiple use cases. Organizations may partner to propose a single use case; however, each organization must submit a letter of interest. There may be continuing opportunity to participate even after initial activity commences for participants who were not selected initially or have submitted the letter of interest after the selection process.

When the project has been completed, NIST will post a notice on the *Accelerate Adoption of Digital Identities on Mobile Devices* project website at <https://www.nccoe.nist.gov/projects/digital-identities-mdl> announcing the next phase of the project and informing the public that it will no longer accept letters of interest for this

project. Selected participants will be required to enter into an NCCoE consortium CRADA with NIST (for reference, see **ADDRESSES** section above).

Project Objective: Digital identities are supplementing and supplanting traditional physical identity cards. Customers, consumers of services, law enforcement, vendors, suppliers, businesses, and health care entities may require a method of verifying a person via a mobile device. If these digital identities on mobile devices are to meet the demands of varying use cases, there must be technological interoperability, security, and cross-domain trust. The nascent nature of this technology leaves many challenges to be addressed, including but not limited to:

- Lack of guidance and governance for identities on devices
- Limited capability to evaluate and validate compliant, standards-based deployments
- Limited understanding of the privacy and usability considerations

The goal of this project is to define and facilitate a reference architecture(s) for digital identities that protects privacy, is implemented in a secure way, enables equity, is widely adoptable, interoperable, and easy to use. The concepts of cybersecurity, privacy, and adoptability are critically important to this overall effort and will be interweaved into the work of this project from the beginning. The NCCoE intends to help accelerate the adoption of the standards, investigate what works and what does not based upon current efforts being performed by various entities, and provide a forum/environment to discuss and resolve challenges in implementing ISO/IEC 18013-5 (attended) and ISO/IEC 18013-7 (over-the-internet) standards.

The scope of this project will include developing an implementable reference architecture for the ISO/IEC 18013-5 and ISO/IEC 18013-7 standard and provide opportunities for validation of use cases. This effort may also consider other standards-based initiatives,

such as emerging efforts around W3C's Mobile Document Request API (GitHub - WICG/mobile-document-request-api) for mobile document (mdoc) presentation.

Specific outcomes of this project will be:

1. Open-Source Reader Reference Implementation – This will be a freely available tool for testing and evaluating compliance of mDL implementations with international standards and will be used as part of the demonstration efforts to confirm interoperability of mDL and mdoc applications for use in the lab.
2. Demonstrations of mDL Use Cases – These will demonstrate end-to-end uses of mDL in attended and over-the-internet use cases. This will include multiple parties such as issuers of mDL, mdoc App providers, digital identity service providers and verifiers (aka, relying parties) that consume mDLs, all collaborating to bring practical uses to life. NCCoE plans to build up to two demonstrations per transaction type. There are five transaction types which are described in Section 4 of the project description.
3. Practice Guide – This will capture the lessons of the demonstrations to provide a usable guide for implementing mDLs in attended and over-the-internet scenarios. This will include design, architecture, integration information inclusive of leading practice for security, usability, and privacy based on the work with our collaborators.

While these standards address the needs of mDLs, many parts of these standards apply to mobile documents in general. Accordingly, this effort will include presentation of documents other than mDLs using the mdoc data model defined in these standards.

Requirements for Letters of Interest:

Each responding organization's letter of interest should include the following information in the description:

1. The organization's role(s) in the project. The choices are:
 - a. Verifier (aka, Relying Party),
 - b. mDL and mdoc App Provider,
 - c. State DMVs or Other Issuing Authority,
 - d. Digital Identity Service Provider, and / or
 - e. Third Party Trust Service Provider.
2. Verifiers should provide a brief description of each use case being proposed.
3. Document Type(s) the product supports.

Letters of interest should not include company proprietary information, and all components and capabilities must be commercially available.

The NCCoE is inviting organizations who have implemented or are planning to implement ISO/IEC 18013-5 and ISO/IEC 18013-7 (draft) standards to collaborate and contribute toward building mDL (also other document types) demonstrations in the NCCoE lab. The following are NCCoE expectations of different types of participants:

- Verifiers are expected to bring use cases and business processes with use cases that
 - Already support mDL / mdoc functionality,
 - Are willing to work and integrate with digital identity service providers to mDL / mdoc-enable their use case, or
 - Are willing to integrate NIST open-source reader reference implementation to mDL / mdoc-enable their use case.
- mDL / mdoc App providers are expected to meet the minimum requirements as specified in Section 2 of the project description
- mDL / mdoc Issuers are expected to provide Test mDLs / mdocs
- Digital Identity service providers are expected to provide integration services

- Third-Party Trust Service Providers are expected to provide Verified Issuer Certificate Authority List (VICAL)

Additional details about the *Accelerate Adoption of Digital Identities on Mobile Devices* project are available at <https://www.nccoe.nist.gov/projects/digital-identities-mdl>.

NIST cannot guarantee that all submissions will be used, or that the products proposed by respondents will be used in a demonstration. Each prospective participant will be expected to work collaboratively with NIST staff and other project participants under the terms of the NCCoE consortium CRADA in the development of the *Accelerate Adoption of Digital Identities on Mobile Devices* project. Prospective participants' contributions to the collaborative effort will include assistance in establishing the necessary interface functionality, connection and set-up capabilities and procedures, demonstration harnesses, environmental and safety conditions for use, integrated platform user instructions, and demonstration plans and scripts necessary to demonstrate a use case. Each participant will work with NIST personnel and other participants, as necessary, to integrate their solution into a demonstration of a use case. Following successful demonstration, NIST will publish a description of each demonstration that includes information such as server architecture, device architecture, usability considerations, performance characteristics, and lessons learned that meets the security and privacy objectives of the *Accelerate Adoption of Digital Identities on Mobile Devices* project. These descriptions will be public information.

Under the terms of the NCCoE consortium CRADA, NIST will support development of interfaces among participants' products by providing IT infrastructure, laboratory facilities, office facilities, collaboration facilities, and staff support to component composition, security platform documentation, and demonstration activities.

The dates of the demonstration of *Accelerate Adoption of Digital Identities on Mobile Devices* project capability will be announced on the NCCoE website at least two weeks in

advance at <https://www.nccoe.nist.gov/projects/digital-identities-mdl>. The expected outcome will demonstrate how the components of the *Accelerate Adoption of Digital Identities on Mobile Devices* project architecture can provide security and privacy capabilities to mitigate potential risks to digital identities throughout their lifecycle. Participating organizations will gain from the knowledge that their products are interoperable with other participants' offerings.

For additional information on the NCCoE governance, business processes, and NCCoE operational structure, visit the NCCoE website <https://nccoe.nist.gov/>.

Alicia Chambers,

NIST Executive Secretariat.

[FR Doc. 2023-18591 Filed: 8/28/2023 8:45 am; Publication Date: 8/29/2023]